**Technology Usage Policy**

*Last Updated: 11/28/2023*

**1. Purpose**

This Technology Usage Policy outlines the guidelines and expectations for the use of technology and information systems at our company. The objective is to ensure the responsible and secure use of company-provided technology resources.

**2. Acceptable Use**

**a. Company-Owned Devices**

* Employees are expected to use company-owned devices, including computers, laptops, tablets, and smartphones, for work-related purposes.
* Personal use of company-owned devices should be limited and comply with the guidelines outlined in this policy.

**b. Software and Applications**

* Employees should only install authorized software and applications on company-owned devices.
* All software installations must be approved by the IT department.

**c. Internet Usage**

* Internet usage should be for work-related purposes only.
* Accessing inappropriate content, downloading unauthorized files, or engaging in activities that pose security risks is strictly prohibited.

**3. Data Security**

**a. Confidential Information**

* Employees must exercise caution when handling confidential company information.
* Confidential information should not be shared with unauthorized individuals, both within and outside the company.

**b. Password Protection**

* Employees are responsible for creating strong and unique passwords for their accounts.
* Passwords should be kept confidential and not shared with others.

**c. Data Backup**

* Regular data backups are essential to prevent data loss.
* Employees should save work on network drives or cloud-based solutions provided by the company.

**4. Security Measures**

**a. Antivirus and Anti-Malware**

* All company-owned devices must have up-to-date antivirus and anti-malware software installed.
* Employees should report any suspicious activities or security threats to the IT department.

**b. Device Security**

* Company devices should be secured with passwords, PINs, or biometric authentication methods.
* Lost or stolen devices must be reported immediately to the IT department.

**c. Remote Access**

* Remote access to company systems should be done through secure and approved methods.
* Employees should not use public Wi-Fi for accessing sensitive company information.

**5. Communication Security**

**a. Email**

* Employees should exercise caution when opening emails from unknown sources.
* Confidential information should not be sent via email unless encrypted.

**b. Instant Messaging and Collaboration Tools**

* The use of instant messaging and collaboration tools for work-related communication is encouraged.
* Employees should follow company guidelines for secure communication on these platforms.

**6. Compliance**

* All employees must adhere to local and international laws related to technology use.
* Violations of this policy may result in disciplinary action, up to and including termination of employment.

**7. Reporting Security Incidents**

* Employees should promptly report any security incidents, including suspected data breaches or unauthorized access, to the IT department.

**8. Review and Updates**

* This Technology Usage Policy is subject to periodic review and updates.
* Employees will be notified of any changes to the policy.

**9. Contact Information**

If you have questions or concerns regarding this Technology Usage Policy, please contact the IT department at [ITSupport@email.com](mailto:ITSupport@email.com).

By using company technology resources, employees agree to comply with the terms outlined in this policy.

[Company Name]  
[Company Address]  
[San Antonio, TX. 78216]  
[[contact@email.com](mailto:contact@email.com)]